Security Concerns of new alternative telecommunication services

Arbnora Hyseni
University for Business and Technology

Krenare Pireva
University for Business and Technology, krenare.prieva@ubt-uni.net

Miranda Kajtazi
Lund University, miranda.kajtazi@ics.lu.se

Security Concerns of new alternative telecommunication services

Arbnora Hyseni[1], Krenare Pireva[1], Miranda Kajtazi[2,3]

[1]UBT – Higher Education Institution, Prishtina, Kosovo
[2]Lund University, Lund, Sweden
[3]Örebro University, Örebro, Sweden
krenare.prieva@ubt-uni.net[1], miranda.kajtazi@ics.lu.se[2,3]

Abstract. With the advancing new era of communication, the so-called era of 'being always online' many providers offer their services for free. In that sense a small company or a virtual company becomes a huge competitor for different traditional telecommunication providers. Using the same services such as: voice calls, video calls, chat and similar services, the internet technology has made huge changes how users make use of such services . Instead of using these services, users shall install applications that are specialized for offering these services via applications, such as: Viber, WhatsApp, Facebook, Google Talk etc.. During the installation and update of these applications people do not recognize the risks of security and privacy of the information that makes their business vital, and how such information are abused on the fly and reused for unauthorized purposes. Using qualitative and quantitative methods we have conducted an empirical study focused on the usage of "these" services and we have elaborated further the need for increasing the knowledge of people in the area of security and privacy while using "free" services. This paper will highlight the challenges by setting a number of privacy and security concerns that are violated while using "free" online services, also offering a bird's eye view of numerous recommendations developed by various standard organizations.

Keywords: Viber, Skype, Facebook, information security, information privacy, online services.

1. Introduction

Telecommunication, as an industry with tremendous changes due to the ongoing evolutions in technology has experienced new area of communication services, through different open and free service providers. These providers are offering free apps, through which people could establish voice and video calls, messages, conference calls etc. The recent generation of service and application companies known as using the "Internet Over-the-Top services (OTT)" networking as a platform for their service offerings [1]. Companies, such as Skype, Viber, Facebook messenger, WhatsApp, and many others, have emerged to address the new and perceived communications needs of both consumer and enterprise users [2].

The mobility of smart devices, and the upgrade of mobile networks to 3G, HSPA+, LTE services and wireless broadband services, enabled people to be online, most of their time with higher transfer rates. This advancement, has increased the usage of alternative telecommunication providers, who offer their infrastructure for free. All of these application use the VoIP standard, for sharing their real-time traffic through Internet. Such new free communication applications are Viber, Skype, Facebook, Whatsapp etc.

WhatsApp Inc. [3] was founded in 2009 in Santa Clara, California. It is an application which allowes users to exchange voice, text and multimedia messages through their services. WhatsApp is adaptable and can work properly in different platforms such as: iPhone, BlackBerry, Android, Windows, and Nokia etc. It uses Internet for communication

Skype Inc. [3] was founded in 2003, it offers free and commercial services through a single account. It offers different services, such as chatting, calls, video calls and video conferences, sharing the screen etc. Their services are also used for education and business purposes, which are using as part of their everyday work. The application is compatible with different platforms, such as Microsoft, Linux, BlackBerry, iOS, Symbian, Android etc.

Viber [3] was founded in 2010. It is used from more than 606 million people worldwide. It offers services for calls, video and messaging. It is offered in different platforms, such as iOS, Windows, Android, Symbian etc
Facebook [4] was founded in 2004, in Massachusetts. It launched its new services in Facebook messenger. It adds video calls, application called Facebook Messenger for chatting and calling as a new services for communicating peer to peer.
Within this paper, we are trying to identify some of the "hidden" activities within these applications and explore how the users are using this applications, for what purposes and do they concern for their data security and privacy.

2. Privacy concerns and identification of new challenges

With the advancement of new era of technology, being able to be online most of the time, there are many different providers who are offering their services for "free" for telecommunication purposes. In this context, many small companies, with a small number of employees, are becoming real competitors with huge public and private telecommunication companies, who are in the same business area. Example, WhatsApp started with 5 employees its business idea, and now is one of the world competitors in the telecom industry with 700 million users world-wide. On June, 2013, they announced a new record by processing 27 billion messages in one day [3].
Many users, while using these applications that are being offered as "free", are scarifying their personal data, as a paying back the use of their services, where most of the people are not aware of.
Lately, there are raised many privacy concerns while installing these apps, that their data are being used and reused for unauthorized purposes. While being installed each of the apps required access to users contact list, so they could discover who is using the app and connect them directly. So in that case, the contact list was mirrored in their server, including contact information for contacts who are not using these apps [3]. Some of the apps required even access on messages, galleries etc. In article [5], there were a comparison between different alternative providers, based on a specific criteria, which is shown in table 1. Such criteria as: **Criteria 1:** Does the encryption apply while data are transmitted; **Criteria 2:** Does your communication is encrypted with any key that the provider could not have access on your data
Criteria 3: Could the contact identities be verified? **Criteria 4:** Are your past discussion secure, if your security is broken? **Criteria 5:** Is the code open to independent review? **Criteria 6:** Is there a documentation for security steps? **Criteria 7:** Has there been a code audit?

Table 1: Comparison of apps based on 7 Criterias

Application	C_1	C_2	C_3	C_4	C_5	C_6	C_7
Viber	Yes	No	No	No	No	No	No
WhatsApp	Yes	No	No	No	No	No	Yes
Skype	Yes	No	No	No	No	No	No
Facebook Messenger	Yes	No	No	No	No	No	Yes

So in this context, most of the providers instead of protecting their uses privacy, implemented end-to-end and transport layer encryption, which are meant to make eavesdropping infeasible even for the service providers themselves, whereas most of the other criterias' are neglected [10]. Many security holes where identified last year's, Whatsapp faced a problem in the first verion of their apps when the communication was not encrypted, second security hole was reported which left the users accounts open for session h*ijacking and packet analysis[1]*. *However in viber on* July 24, 2013, Viber's support system was defaced by Syrian Electronic Army, which then was reported from viber that no information was accessed.

3. Methodology

In this research paper we used quantitative method for getting the opinion of the users, analyzing the actual situation in usage of alternative telecommunication services and how the users are being concern for their data

privacy. Data within this research paper are conducted through questionnaires, from four different Universities and then analyzed and presented further in the result section.
In the questionnaires have participated totally 200 students, from different level of education. Most of the students are with Computer Science background, which could have an impact on the general results.

4. Results and Discussions

In order to identify how often the users are using the alternative services, and what are the purpose of using these services from the companies that are offering their application for free, and if they are aware of the payment back option.
Below are listed some of our graphs and description of our research results done thru couple of questions.
For the question: Do you have knowledge regarding new alternative communication services (Viber, Skype, WhatsApp, Facebook etc)

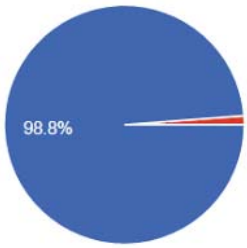


Fig 1. Having knowledge of alternative communication services

A 98.8 percent of the users answered with yes, and they already use one of them.
For the question: For whatever purposes do you use them?

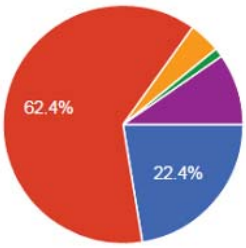


Fig 2. Purpose of using alternative communication services

The users declared that 62.4% they used for communicating with friends, followed by 22.4% talking to their families and relevant.
In the following question, Which of these application do you use more often for the purposed declared on the previous question?

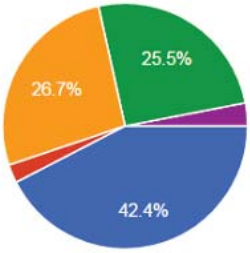
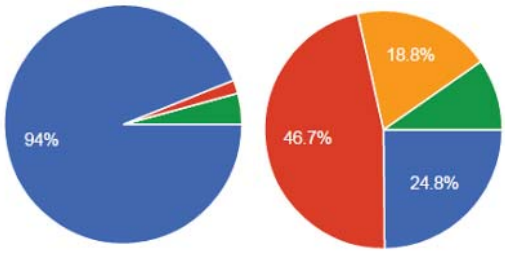


Fig 3. Using one of alternative communication services

From all participated users, 42.4% used Viber, 26.7% WhatsApp, followed by Facebook with 25.5%.
In the questions: (a) How often do you use the alternative services before the traditional options, and (b) Why do you use them?



(a) (b)

Fig 4. (a) The use of alternative services before traditional option, and (b) Why using it

For (a) 94 % of users used the alternative services instead of traditional options, whereas for (b) 46.7.5% of them use because of the low cost, followed by quality and habit.
And in the most important part of our research, we were trying to get the information if the users concern for their data privacy, for their personal data and also for the traffic that was exchanged. And, 72.9% of them expressed that they do concern, but it's a cheaper alternative for generating international and local calls, followed by 25.9 % of the users that don't consider at all the privacy issue, as shown in the Fig 5.

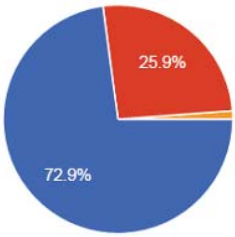
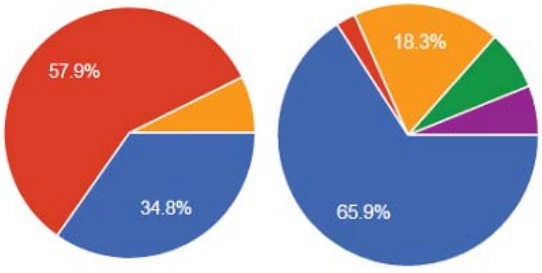


Fig 5. The concern of data privacy and security while using free services

And, the final questions: Have you ever doubt on these services for your data privacy and security? And would you be aware for techniques that will increase the data privacy and security. Surprisingly, in (a) 57.9% of users declared that they have doubts on which data are having access the providers and how they use, whereas in (b), 65.9% of the users showed interests in gaining knowledge for increasing the knowledge in awareness techniques.



(a) (b)

Fig 6. (a) Doubts about the use of our personal data, and (b) Awareness of using techniques for enhancing the security of data.

Conclusion

New alternative application for communication are valuable apps and marketing tools. In these applications are different security risks which could also not be omitted in traditional telecommunication services. However

in this direction users are given permission to different authorized and not authorized providers to have access on their data, violating their privacy and their own security for using their so called “free” services. As discussed in the last section many users, even that they have doubts on those providers 57.9%, they continually use their services with 94%, without trying to prevent any security breakage or even to protect their data by implementing different encryption techniques that could increases the data security.

References and Bibliography

1. Terry Matthews, “Over-The-Top (OTT) A Dramatic makeover of Global Communications “, Wesley Clover International, 2014
2. Nuqi, Florian, Pireva Krenare, and Efstathiadis, “The impact of new alternative telecommunication services on the strategy of traditional telecom providers in Kosovo” , IC-CSCE 2014, Durres, Albania
3. Aal, Limbesh B., et al. "Whatsapp, Skype, Wickr, Viber, Twitter and Blog are Ready to Asymptote Globally from All Corners during Communications in Latest Fast Life." Research Journal of Science and Technology 6.2 (2014): 101-116.
4. Jones, Harvey, and José Hiram Soltren. "Facebook: Threats to privacy."Project MAC: MIT Project on Mathematics and Computing 1 (2005): 1-76.
5. Mazurczyk, Wojciech, and Zbigniew Kotulski. "Lightweight security mechanism for PSTN-VoIP cooperation." arXiv preprint cs/0612054 (2006).
6. Mahajan, Aditya, M. S. Dahiya, and H. P. Sanghvi. "Forensic analysis of instant messenger applications on android devices." arXiv preprint arXiv:1304.4915 (2013).
7. Schrittwieser, Sebastian, et al. "Guess Who's Texting You? Evaluating the Security of Smartphone Messaging Applications." NDSS. 2012.
8. Coull, Scott E., and Kevin P. Dyer. "Traffic Analysis of Encrypted Messaging Services: Apple iMessage and Beyond." ACM SIGCOMM Computer Communication Review 44.5 (2014): 5-11.
9. Coull, Scott E., and Kevin P. Dyer. "Traffic Analysis of Encrypted Messaging Services: Apple iMessage and Beyond." ACM SIGCOMM Computer Communication Review 44.5 (2014): 5-11.
10. Ahmar Ghaffar, “How Secure Is VoIP?”, [Online in: http://www.isoc.org/ pubpolpillar/voip-paper.shtml, Accessed on: 12 January 2016]
11. TBU News. (2015). Privacy and Security – Face Viber And BBM not quite Secure Tor And Open Whisper Champions of Security [Accessed on, 12 January 2016]
12. Kierkegaard, Sylvia (2006). "Blogs, lies and the doocing: The next hotbed of litigation?". Computer Law and Security Report 22 (2): 127.